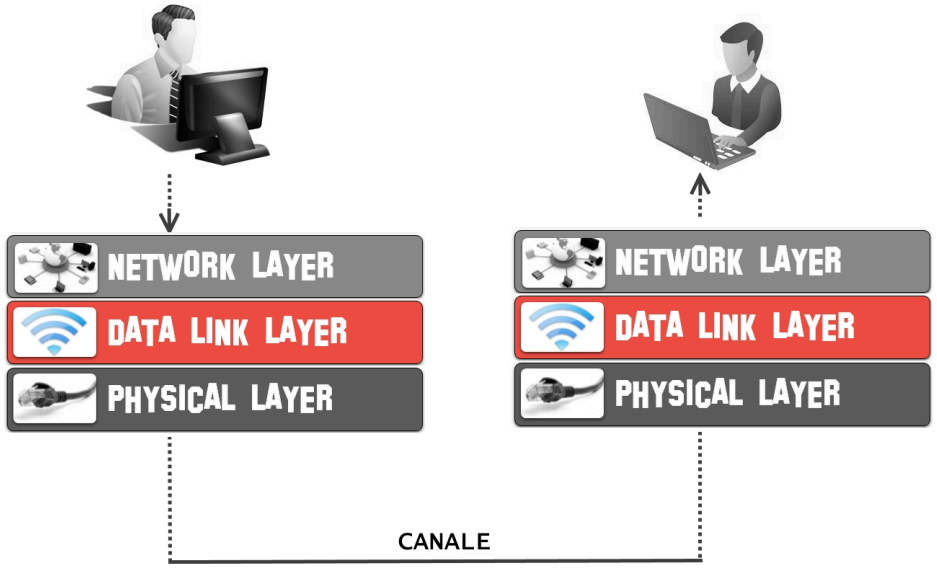
Link Layer

The data link layer, also called the **link layer**, is located below the network layer and above the physical layer.

This layer receives packets from the network layer and encapsulates them into units that are then transmitted through the physical layer.

Its task is to manage communication over a single local link, using rules appropriate to the technology being used, such as Ethernet or Wi-Fi.



The data link layer is responsible for:

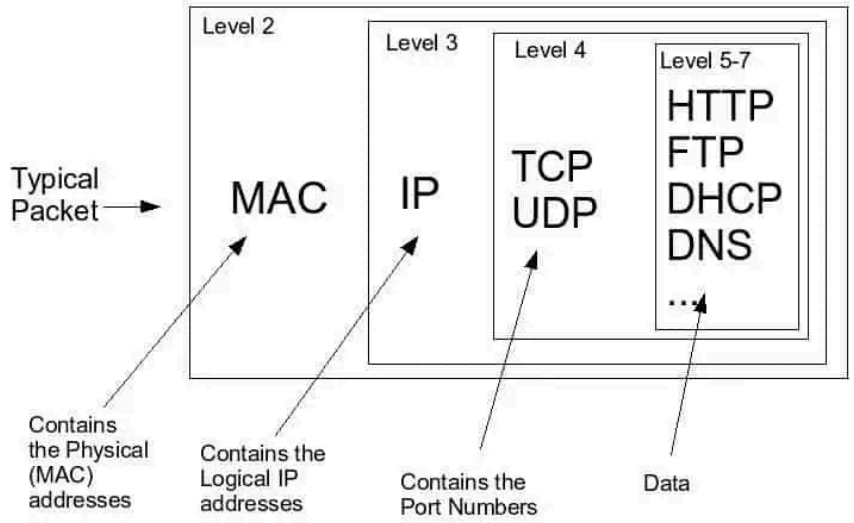
- Organising the raw bits transmitted by the physical layer into readable and manageable units.
- Addressing devices within the local network using MAC addresses.
- Detecting errors in local transmissions:
    - Checking whether data has arrived intact by using error-detection codes, as Ethernet does.
    - Requesting retransmission when errors occur, as some technologies other than Ethernet may do.
- Preventing conflicts and collisions, particularly in shared networks.

One of the most widely used technologies at this layer is **Ethernet**, and its data unit is called a **frame**.

An Ethernet frame is divided into the following parts:

- **Header:** Contains information such as the sender's and recipient's MAC addresses.
- **Payload:** Contains the actual data, such as an IP packet.

- **Trailer:** Contains an error-detection code.



Error Detection

The error-detection value used by Ethernet is called the **FCS**, or **Frame Check Sequence**.

The FCS is a 32-bit value calculated from the contents of the frame using an algorithm called **CRC**, or **Cyclic Redundancy Check**.

- If the value calculated by the recipient matches the value contained in the FCS field, the frame is considered valid.
- If the values do not match, the frame was probably altered during transmission and is discarded.

CRC provides several advantages:

- It detects all single-bit errors, where one incorrect bit appears among otherwise correct bits.
- It detects many multiple-bit errors.
- It detects burst errors, meaning groups of errors concentrated within part of the transmitted data.
- It can be calculated very efficiently, including directly by hardware.

The following process shows how CRC is used by the sender and recipient.

The Sender

- Takes the entire contents of the frame, excluding the FCS field, which will be added later.
- Calculates the CRC from the frame contents.
- Obtains a 32-bit value.
- Inserts this value into the FCS field at the end of the frame.

The Recipient

- Receives the entire frame, including the FCS field.
- Performs the CRC check on the received frame.
- Compares the calculated result with the value contained in the FCS field:
    - If the two values match, the frame is assumed to be valid.
    - If they do not match, the frame is discarded. Ethernet does not provide automatic retransmission. When retransmission is required, it is handled by an upper layer, such as TCP at the transport layer.

The Journey of a Web Request Through a Network

How are packets transmitted from a source host to a destination host?

The following example examines the different stages of a message flow that uses **HTTP** at the application layer. HTTP is the protocol used to request and transfer web pages.

More specifically, we will examine an HTTP request in which a client asks a server for a web page.

Creating the Data Units

The browser generates an HTTP request.

The transport layer uses TCP to encapsulate the HTTP data inside a **TCP segment**.

Network Layer

The TCP segment is passed to the network layer, which encapsulates it inside an **IP packet**.

The packet contains the destination IP address—obtained through DNS from the domain name—and the message payload.

Link Layer

The IP packet is then encapsulated inside an Ethernet frame.

Because the final destination is outside the local network, the destination MAC address in the frame is the MAC address of the gateway.

The host obtains the gateway's MAC address through:

- **ARP** when IPv4 is being used.
- **Neighbour Discovery** when IPv6 is being used.

These mechanisms associate an IP address with a MAC address only on directly connected networks.

Forwarding the Frame to the Gateway

The Ethernet frame containing the packet is transmitted across the local network and reaches the gateway.

The gateway acts as the access point between the local network and the external network—in this case, the Internet.

Routing and Forwarding

The gateway extracts the IP packet from the received frame and examines its destination IP address.

It then consults its routing table to determine the next destination, usually another router, to which the packet must be forwarded.

Finding the Next-Hop MAC Address

Once the **next hop** has been identified, the router obtains its corresponding MAC address using:

- Its ARP table for IPv4.
- Its Neighbour Discovery table for IPv6.

Replacing the MAC Addresses

The router keeps the same IP packet, apart from certain technical modifications, but encapsulates it inside a new link-layer frame suitable for the next connection.

In this new frame, the destination MAC address belongs to:

- The next router; or
- The final host, when it is located on a directly connected network.

Forwarding to the Next Router

The IP packet is placed inside a new Ethernet frame and transmitted to the next router.

That router examines the destination IP address at the network layer and forwards the packet towards another router, using the MAC address required for the next local link.

Repeating the Forwarding Process

This forwarding process is repeated across the chain of routers until the packet reaches the gateway of the destination network.

Delivering the Packet to the Destination Host

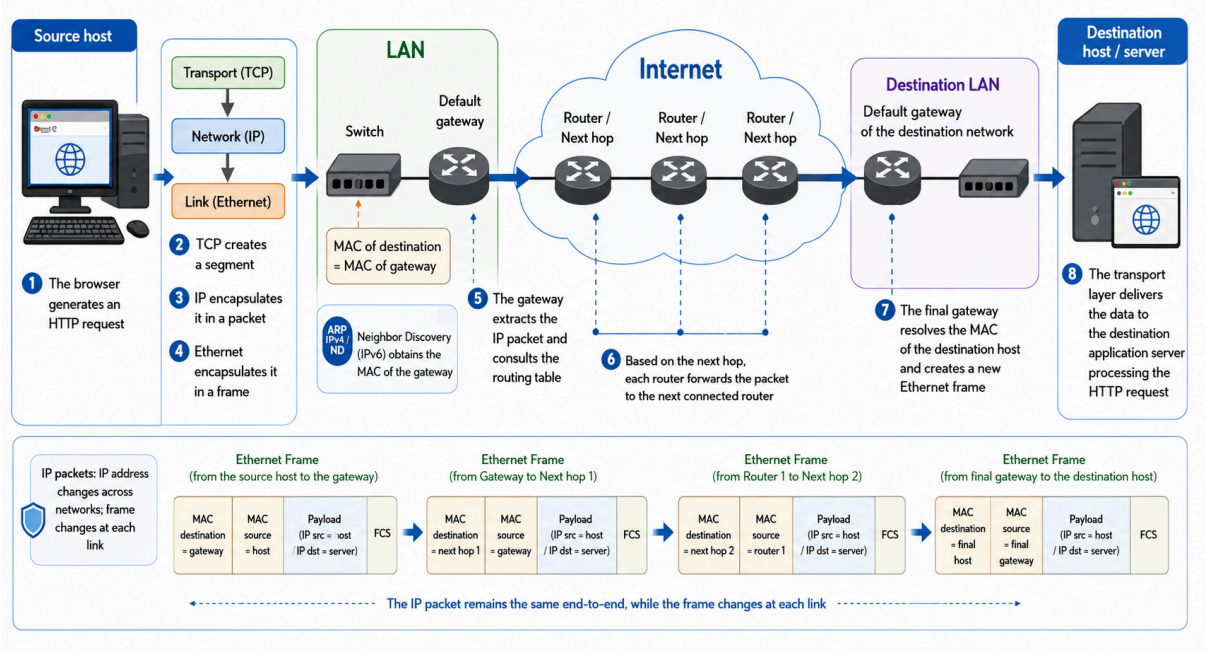
The final gateway receives the frame and extracts the IP packet.

It then creates a new Ethernet frame containing the destination host's MAC address. The gateway can obtain this address through ARP or Neighbour Discovery.

The gateway then forwards the new frame to the destination host within its local network.

Receiving the Request

At the destination, the transport layer reads the destination port contained in the TCP segment and delivers the data to the correct socket and application—in this case, the HTTP server application.



Note: During the journey, the IP packet normally retains the source and final destination IP addresses, while the link-layer frame changes at every network segment.

Each router extracts the IP packet from the frame it receives and encapsulates it inside a new frame suitable for the next link.